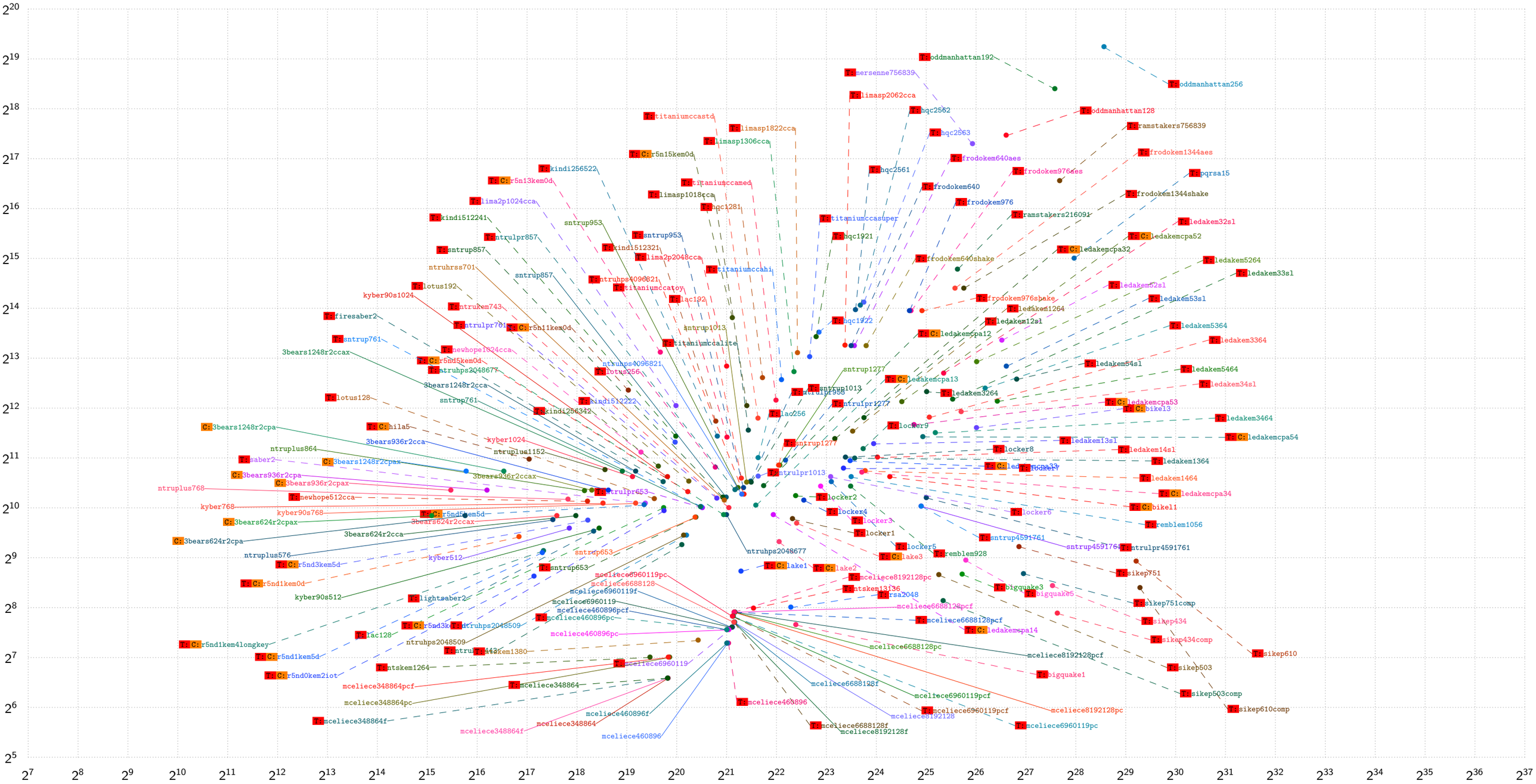
amd64, wolfdale, crypto_kem, dec time, ciphertext size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto_kem_dec). 20240912

Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

"C:" means that the SUPERCOP database does not list IND-CCA2 security as a goal for this primitive. "T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.


2^20
2^19
2^18
2^17
2^16
2^15
2^14
2^13
2^12
2^11
2^10
2^9
2^8
2^7
2^6
2^5
2^7 2^8 2^9 2^10 2^11 2^12 2^13 2^14 2^15 2^16 2^17 2^18 2^19 2^20 2^21 2^22 2^23 2^24 2^25 2^26 2^27 2^28 2^29 2^30 2^31 2^32 2^33 2^34 2^35 2^36 2^37
T: oddmanhattan192
T: mersenne756839
T: oddmanhattan256
T: limasp2062cca
T: hqc2562
T: oddmanhattan128
T: ramstakers756839
T: hqc2563
T: frodokem1344aes
T: frodokem640aes
T: frodokem976aes
T: pqrsa15
T: frodokem1344shake
T: ramstakers216091
T: ledakemcpa52
T: C: ledakemcpa32
T: ledakem5264
T: ledakem33s1
T: ledakem52s1
T: ledakem53s1
T: ledakem5364
T: ledakem3364
T: ledakem54s1
T: ledakem5464
T: ledakem34s1
T: C: ledakemcpa53
T: C: bikel3
T: ledakem3464
T: C: ledakemcpa54
T: ledakem13s1
T: ledakem14s1
T: ledakem1364
T: ledakem1464
T: C: ledakemcpa34
T: C: bikel1
T: cemblem1056
T: ntrulpr4591761
T: sikep751
T: sikep751comp
T: sikep434
T: sikep434comp
T: sikep610
T: sikep503
T: sikep503comp
T: sikep610comp
T: C: ledakemcpa14
T: frodokem640
T: frodokem976
T: frodokem640shake
T: frodokem976shake
T: ledakem1264
T: ledakem12s1
T: C: ledakemcpa12
T: C: ledakemcpa13
T: ledakem3264
T: ntrulpr1277
T: locker9
T: locker8
T: C: ledakemcpa17
T: locker7
T: locker2
T: locker4
T: locker3
T: locker1
T: locker5
T: locker6
T: C: lake3
T: cremblem928
T: C: lake1
T: C: lake2
T: mceliece8192128pc
T: ntskem13136
T: rsa2048
T: bigquake3
T: bigquake5
T: mceliece6688128pcf
T: bigquake1
T: titaniumccastd
T: limasp1822cca
T: limasp1306cca
T: C: r5n15kem0d
T: kindi256522
T: C: r5n13kem0d
T: titaniumccamed
T: limasp1018cca
T: lima2p1024cca
T: hqc1281
T: kindi512241
T: titaniumccasuper
T: hqc1921
T: ntrulpr857
T: sntrup953
T: sntrup857
T: kindi512321
T: lima2p2048cca
T: titaniumccahi
T: ntruhps4096821
T: titaniumccatoy
T: lac192
T: ntrukem743
T: ntrulpr761
T: C: r5n11kem0d
T: hqc1922
T: sntrup1013
T: titaniumccalite
T: sntrup761
T: newhope1024cca
T: C: r5nd5kem0d
T: ntruhps2048677
T: lotus256
T: lotus192
T: lotus128
T: firesaber2
T: kindi512222
T: kindi256342
T: lac256
T: C: hila5
T: saber2
T: newhope512cca
T: C: r5nd5kem5d
T: C: r5nd3kem5d
T: C: r5nd1kem0d
T: lightsaber2
T: C: r5nd3kem
T: ntruhps2048509
T: mceliece460896pc
T: lac128
T: C: r5nd1kem4longkey
T: C: r5nd1kem5d
T: C: r5nd0kem2iot
T: ntskem1264
T: mceliece348864
T: mceliece348864f
T: mceliece6960119
T: mceliece460896
T: mceliece6688128f
T: mceliece6960119pcf
T: mceliece6960119pc
T: mceliece8192128pc
T: mceliece6688128pc
T: mceliece6688128pcf
T: mceliece8192128pcf
T: mceliece8192128f
T: mceliece6688128f
T: mceliece460896f
T: mceliece348864pcf
T: mceliece348864pc
T: mceliece460896pcf
T: mceliece6960119pc
T: mceliece6688128pc
T: mceliece6960119pcf
T: mceliece460896pc
T: mceliece6960119pc
T: mceliece6688128pc
T: mceliece6960119pcf
T: mceliece8192128pcf
T: mceliece8192128pc
T: mceliece8192128f
T: mceliece6688128f
T: mceliece460896f
T: mceliece348864pcf
T: mceliece348864pc
T: mceliece460896pcf